Protection from Low-Rate DDOS (Distributed Denial of Service) using Identity Algorithm

Khan Altab[1] Vimmi Porinchu[2]
[1,2]Masters of Computer Application
[1,2]ASM College, Thane, Maharashtra India

Abstract— The modern internet technology has many gateways where attackers can access the service through number of devices. In this generation there is lots of attack involved in data theft or server crash. The DDos attacks are generated in low level which has been identified as negligible but has higher impact in the performance. When the Distributed Denial of Service attack is performed for bringing the target down by the attacker, is considered as a Low Rate Distribution of Service and it is difficult to specify the legalized traffic and malicious traffic. In this research a new identity algorithm is implemented to stop the Low-rate DDOS attacks. The identity algorithm identifies whether the number of entry of user cross more than five times to the same sever, then the user will be mark as an attacker .The proposed algorithm generates higher efficient result in the mitigation of low rate DDos attacks and improves the network performance.

Key words: DDOS (Distributed Denial of Service), Identity Algorithm

I. INTRODUCTION

The world is associated with each other through internet, utilizing the different devices. Such a large network gets influenced by various attacks day by day. Today, a large scale DDos attack is a highly noticeable event impacting an entire online user base. One common trick of ddos attack, is that attacker or attackers, thwart access to virtually anything: servers, devices, services, networks, applications, and even specific transactions within applications .This is achieved, when attackers sends high inflow of malicious data or requests to the server or website, causing widespread disruption to the system or website. This impact could range from a minor annoyance from disrupted services to experiencing entire website, application, or even entire business taken offline.

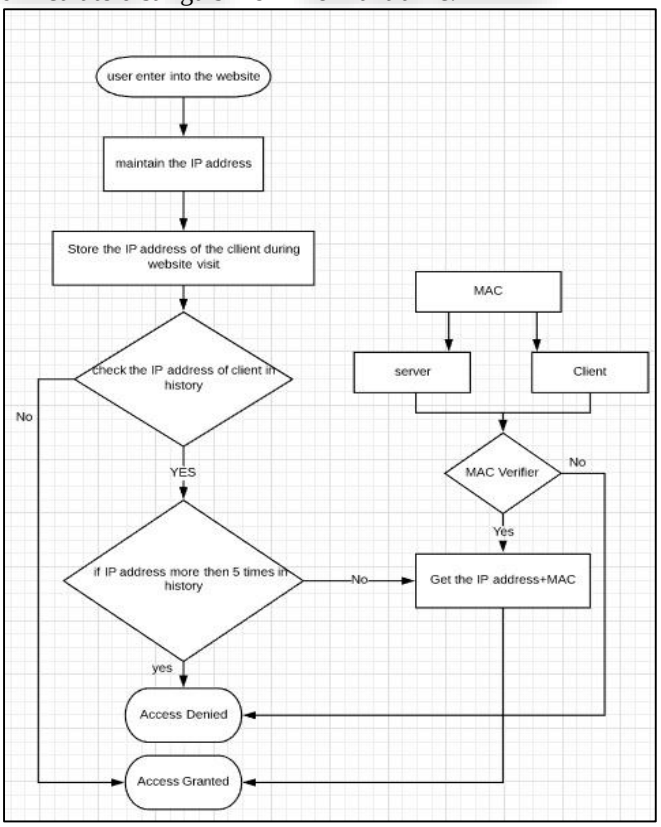
A Low Rate DDos attack is an intelligent attack, as the attacker can send attack packets similar to legitimate traffic to the victims. Low-rate DDoS attacks are different from the traditional DDoS attacks, as their traffic is similar to legitimate traffic. A low-rate DDoS attacker exploits the vulnerability of TCP's(transmission control protocol) congestion-control mechanism by periodically sending burst attack packets over short periods of time repeatedly or back to back sending launching attack packets at a constant low-rate (constant attack). As these types of attacks reduce the average number of attack packets to avoid being detected by the existing detection systems, it is difficult to distinguish such attacks from genuine user and attackers.

II. EXISTING

The existing DDoS attack-detection metrics can be defined into two categories: signature-based metrics and anomaly-based metrics. Signature-Based metrics: in this different type of attack patterns are stored in the database. in this the incoming request is compared with signature database .When suspicious attack is detected a false alarm ring. The signature-based metrics depend on the matching of special patterns to the tested traffic. On the other hand, Anomaly-Based detection :Depends on identifying obvious statistical anomalies by comparison against the legitimate traffic .Entropy is commonly used in anomaly-based metrics .The limitation is that the value of the entropy gap is quite small, which could raise a lot of fake alarms. the anomaly-based detection methods rely on identifying obvious statistical anomalies by comparison against the legitimate traffic. Entropy (lack of prediction or disorder) is commonly used in anomaly-based metrics. The entropy modification(slight difference) between normal traffic and tested traffic may indicate that the entropy value of the tested traffic is anomalous(abnormal) and that's why, low-rate DDoS attack is occurring. However, the limitation is that the value of the entropy gap is quite small, which could raise a lot of fake alarms.

III. PROPOSED METHODOLOGY:

Existing system is not able to differentiate between low rate DDoS attack and the genuine user, as the attacker's traffic is similar to legitimate traffic.Unlike more traditional DDos attack, the low rate attack require very little bandwidth and can be hard to mitigate, as they generate traffic that is very difficult to distinguish form normal traffic.



All rights reserved by www.ijsrd.com

Low rate DDoS attack,act like a genuine user as the attackers send a large amount of attack packets similar to normal traffic, to throttle legitimate flows. In this Proposed methodology, to stop the above problem we apply the identity algorithim that helps to block the attackers. This methods blocks the user who cross the limit of access on particular website ,server or application. Identity algorithm store the IP address of user or attackers and when the user exceed the limit of access then system block that particular use.

IV. IDENTITY ALGORITHM

Start the Process
H=Maintain the IP address History;
U=User enter into the website;
I=Store the Each Client IP address;
Check each time U in server, If (I==H)
{
Else If (I<5)
{
IP=Get the IP address;
MAC 1=IP+MAC
Client=MAC1; If (I<5)
{
Accept the request from the client Send the response for the request.
}
Else
{
Add the User.IP to the Attacker List, Print : “Access Denied”
}
}
}
Else
{
Accept the request from the IP Send the response for the request.
}
End

V. CONCLUSION

The world is increasing digitally day by day. Everyday devices are connected more and more with the Internet. In such a way, the network security becomes more important feature. As network might can get affect by different types of attacks. DDoS at a low rate attack damage the network in a silent manner without getting any notification to the user. It affects the output of TCP applications. And in a network, many applications run within the TCP protocol. This papers describes the techniques of detecting the LDDoS using the identity algorithm.

REFERENCE

[1] Zhang, Changwang, et al. "RRED: robust RED algorithm to counter low-rate denial-of-service attacks." IEEE Communications Letters 14.5 (2010).
[2] Xiang, Yang, Ke Li, and Wanlei Zhou. "Low-rate DDoS attacks detection and traceback by using new information metrics." IEEE Transactions on Information Forensics and Security 6.2 (2011): 426-437.
[3] Ma, Li, Jie Chen, and Bo Zhang. "Improved RED Algorithm for Low-Rate DoS Attack." Advances in Electronic Commerce, Web Application and Communication (2012): 311-316.
[4] Bhuyan, Monowar H., Dhruba Kumar Bhattacharyya, and Jugal K. Kalita. "Information metrics for low-rate DDoS attack detection: A comparative evaluation." Contemporary Computing (IC3), 2014 Seventh International Conference on. IEEE, 2014.
[5] Arora, Arsh, and Lekha Bhambhu. "Performance Analysis of RED & Robust RED." International Journal of Computer Science Trends and Technology (IJCST) 2.5 (2014): 51-55.

All rights reserved by *www.ijsrd.com*